What is HACIENDA?

- Data reconnaissance tool developed by the CITD team in JTRIG
- Port Scans entire countries
  - Uses nmap as port scanning tool
  - Uses GEOFUSION for IP Geolocation
  - Randomly scans every IP identified for that country

Countries

- Completed full scans of 27 countries including
  - [redacted]
- Completed partial scans of 5 additional countries

[redacted]

Tasking & Access

- To task HACIENDA with a Country or Subnet
  - [redacted]@gchq.gov.uk)
  - CITD alias ([redacted]@gchq.gov.uk)
- Access to the Data
  - At GCHQ, request a GLOBAL SURGE account from [redacted]@gchq.gov.uk)
  - At CSEC, contact
  - At NSA, contact
  - At DSD, contact

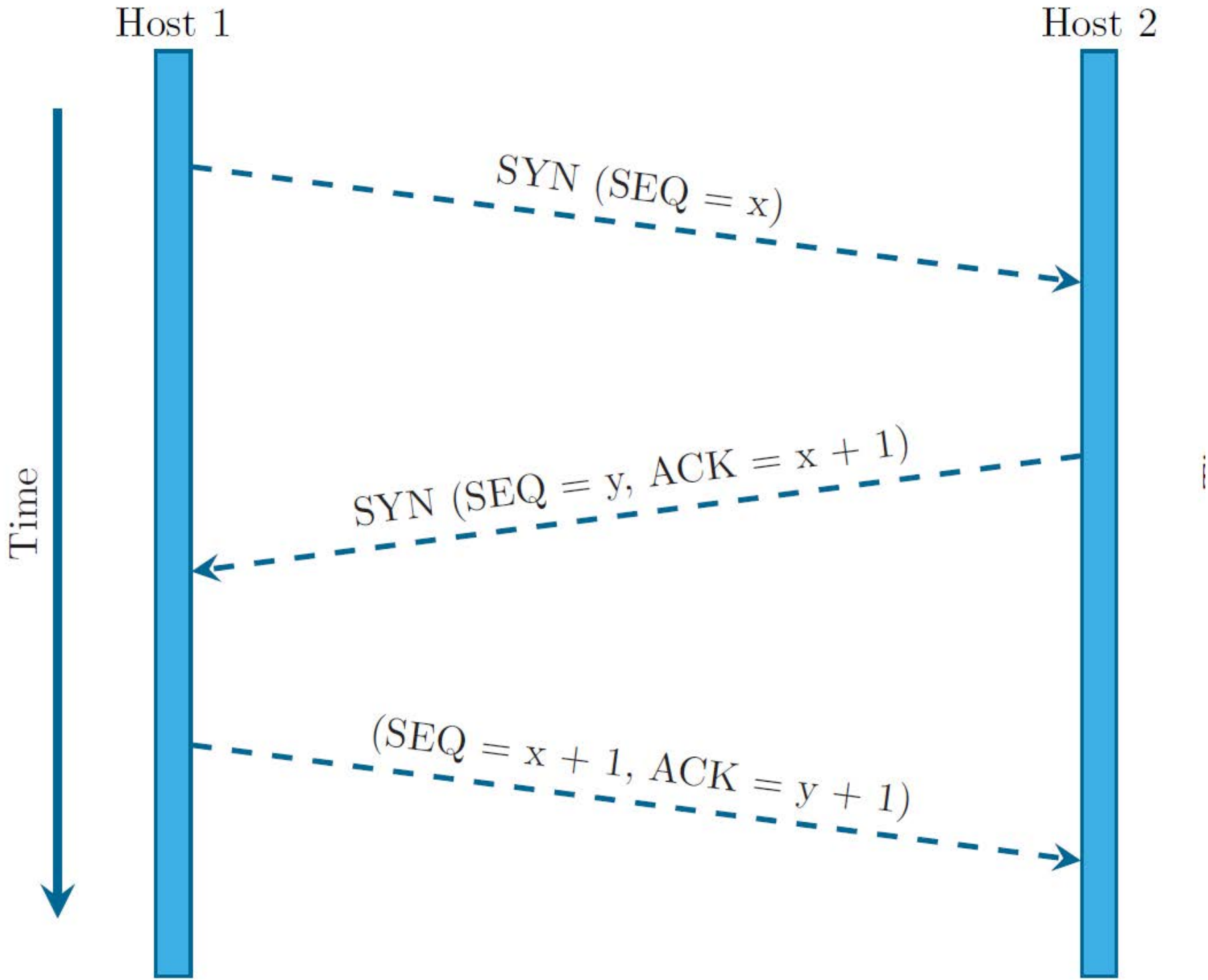
NAC
NETWORK ANALYSIS CENTRE

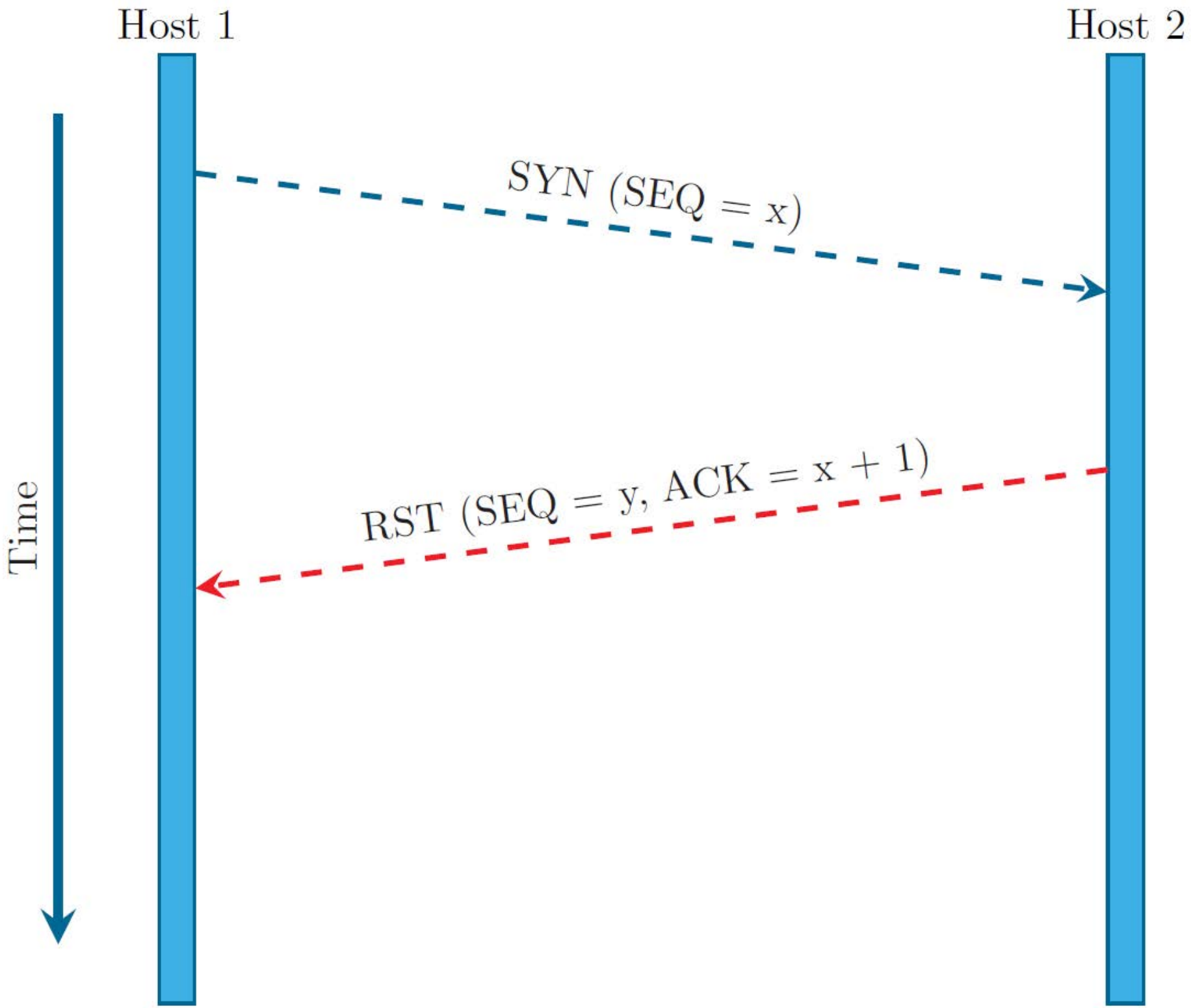
[redacted]

Ports

- Pulls back hostname, banners, application names and port status
- Gathers additional information for…
  - 21 (ftp): directory listing
  - 80 (http): content of main page
  - 443 (https): content of main page
  - 111 (rpc): results of rpcinfo

NAC
NETWORK ANALYSIS CENTRE


Host 1
Host 2
Time
SYN (SEQ = x)
SYN (SEQ = y, ACK = x + 1)
(SEQ = x + 1, ACK = y + 1)


Host 1
Host 2
Time
SYN (SEQ = x)
RST (SEQ = y, ACK = x + 1)

The Results…

- All stored in JTRIG's internal database
- Available in GLOBAL SURGE
  - NAC's Network Knowledge Base Prototype
- Transferred by MAILORDER to
  - CSEC
  - DSD
  - NSA NTOC

NAC
NETWORK ANALYSIS CENTRE

How is it used?

- CNE
  - ORB Detection
  - Vulnerability Assessments
- SD
  - Network Analysis
  - Target Discovery